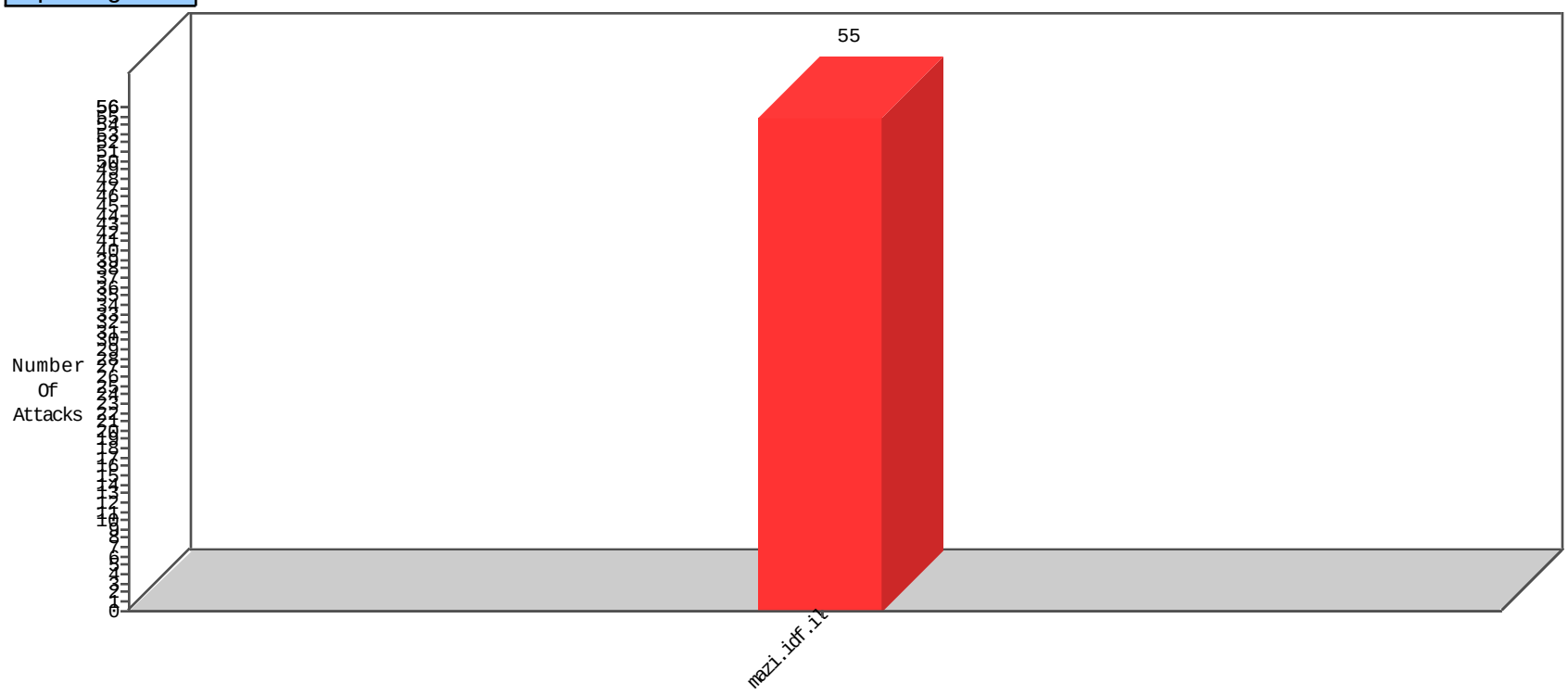
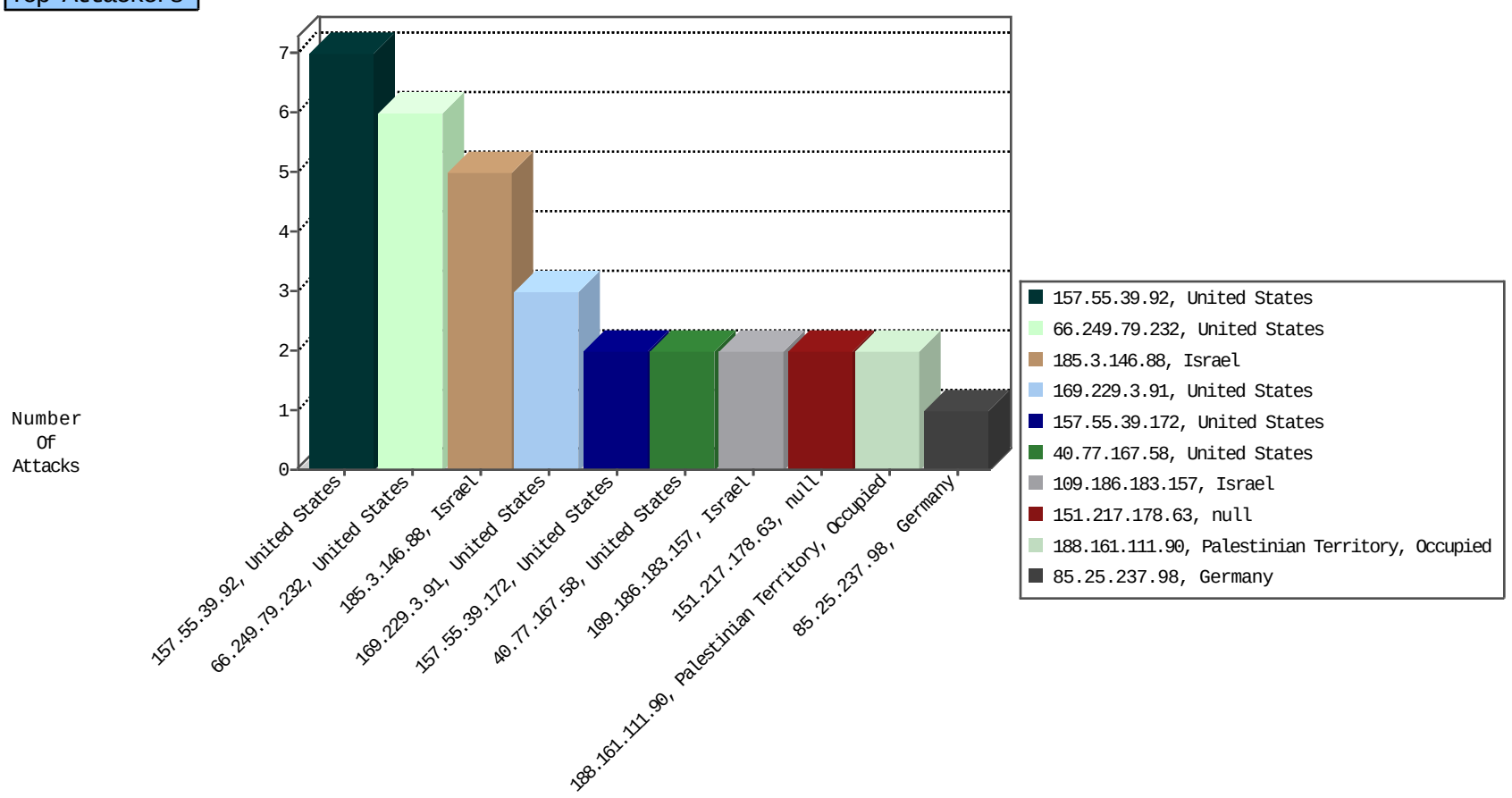
12-28-2015 to 12-29-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-28-2015 to 12-29-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

12-28-2015 to 12-29-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-28-2015 to 12-29-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.79.232	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	6
185.3.146.88	Israel	147.237.77.17	mazi.idf.il	INDICATOR-SCAN myscan	2
151.217.178.63		147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
185.3.146.88	Israel	147.237.77.17	mazi.idf.il	GPL SCAN myscan	2
151.217.178.55		147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88		147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.101.206.244	United Kingdom	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
138.219.176.241		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
218.104.49.211	China	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
94.102.48.195	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

12-28-2015 to 12-29-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
128.127.107.123	Netherlands	147.237.77.17	mazi.idf.i	drop		drop	529
80.246.130.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	100
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	90
46.19.85.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
84.109.18.244	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
37.26.146.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
84.108.80.20	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
37.26.146.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	17
46.19.85.69	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.69	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.117.196.125	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.186.183.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
213.57.131.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
213.57.131.131	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
192.0.80.167	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
213.57.131.131	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
80.246.130.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
128.127.107.123	Netherlands	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
77.125.146.216	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.186	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.236.11	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
2.52.182.222	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.183.29.81	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.207	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.142.236.11	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.59.190	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.161.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.59.38	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
37.26.147.183	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.121.250.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.137.137	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.146.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
85.65.59.38	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.204	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.64.13.83	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.0.81.17	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.186.183.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
62.0.42.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
218.22.211.69	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.0.80.139	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
213.57.137.137	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
62.0.42.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
46.120.185.108	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

12-28-2015 to 12-29-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
157.55.39.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/watch_fragments_ajax	Block	3
109.186.183.157	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
188.161.111.90	Palestinian Territory Occupied	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
185.3.146.88	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/4085-he/igf.aspx	Block	1
157.55.39.172	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 157.55.39.172	Block	1
66.249.79.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6368-9590-he/igf.aspx	Block	1
40.77.167.58	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1
157.55.39.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/count.php	Block	1
77.237.146.28	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
157.55.39.172	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/api/posts/102121/related/more_like_this	Block	1
141.212.122.97	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /x	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
62.0.42.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	NULL Character in Method	Block	1
157.55.39.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/lwes/impression	Block	1
82.80.193.244	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.79.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
207.46.13.21	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
157.55.39.174	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/envivo/json	Block	1
157.55.39.92	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 157.55.39.92	Block	1
77.75.76.168	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
178.83.244.141	Switzerland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
85.25.237.98	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.79.239	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
207.46.13.168	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-11701-he/Ã–Â©Ã–Â¢Ã–Âª Ã–Â? Ã–Â©Ã–Â“ Ã–â€?Ã–â€ºÃ–Â¡Ã–â€¢Ã–Â¤Ã–â„¢Ã–Â?.aspx	Block	1
40.77.167.58	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
157.55.39.92	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
77.75.78.171	Czech Republic	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1

12-28-2015 to 12-29-2015